IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

BRIAN HUDDLESTON,

Plaintiff,

v.

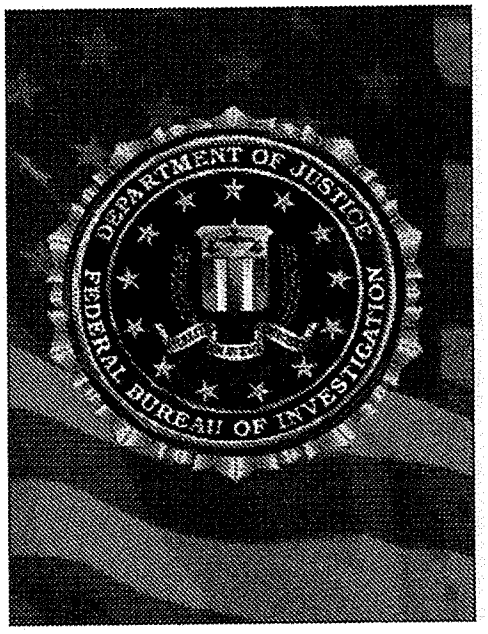
FEDERAL BUREAU OF INVESTIGATION and UNITED STATES DEPARTMENT OF JUSTICE,

Defendants.

CIVIL ACTION No. 4:20CV00447

EXHIBIT C

Records Management Policy Guide



Federal Bureau of Investigation

Records Management Division

0769PG

June 04, 2015

Revised: 07/01/2015

General Information

Questions or comments pertaining to this policy guide can be directed to:

Federal Bureau of Investigation Headquarters (FBIHQ), Records Management Division (RMD)

Records Policy and Administration Section (RPAS), Policy, Analysis, and Compliance Unit (PACU)

Supersession Information

See Appendix E of this policy guide for supersession information.

Table of Contents

List of Appendices

1. Introduction

1.1. Overview

All Federal Bureau of Investigation (FBI) personnel create, maintain, and use FBI records. It is therefore critical that FBI personnel understand the policies and procedures governing the FBI's Records Management Program.

1.2. Recordkeeping Requirements Policy

The FBI is required by law (Title 44 United States Code [U.S.C.] Chapter 31) to establish and implement agencywide programs to identify, develop, issue, and periodically review recordkeeping requirements for records of all agency activities at all levels and locations and across all media.

Recordkeeping requirements provide the regulatory means to implement adequate and proper documentation requirements. They provide specific instructions developed by subject matter experts for the collection of information or the maintenance of documents for FBI functions or programs. Recordkeeping requirements can range from broad, governmentwide guidance found in statutes and regulations to office-specific instructions on the preparation of a certain report. Each FBI Headquarters (FBIHQ) division, field office (FO), and legal attaché (Legat) office must, with the assistance of the Records Management Division (RMD), incorporate applicable laws, regulations, or other requirements pertinent to the organization's program responsibilities into recordkeeping requirements for the documentation of its programs.

1.3. Purpose of Records Management

The RMD's mission is to ensure that the right records are created, made available to the right people at the right time and for the right reasons, and disposed of, according to the disposition authorities approved in the FBI Records Retention Plan.

FBI records must be adequate, authentic, legally sufficient, and secure to ensure all FBI legal, fiscal, administrative, and business needs are met. Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, effectively perform its critical missions, or efficiently conduct its day-to-day business.

The FBI is committed to ensuring its Records Management Program:

- Supports law enforcement and national security operations.
- Facilitates documentation of official decisions, policies, activities, and transactions.
- Facilitates timely retrieval and sharing of needed information.
- Ensures business continuity.
- Controls the creation and growth of FBI records.

- Reduces operating costs by managing records according to the FBI's business needs and by encouraging appropriate disposition practices pursuant to the FBI Records Retention Plan.
- Improves efficiency and productivity through effective records storage and retrieval methods.
- Ensures compliance with applicable laws and regulations.
- Safeguards the FBI's mission-critical information.
- Preserves the FBI's history.
- Implements technology to support records management activities.

1.4. Benefits of Good Recordkeeping

Adequate and proper recordkeeping ensures that information is available to safeguard the legal and financial rights of the federal government, the FBI, and persons directly affected by the FBI's activities. It ensures the accountability of the FBI to the President of the United States, the United States Congress, the United States courts, and the American people. Additionally, it supports the administration of justice and effective law enforcement and national security operations throughout the FBI's worldwide operations.

Conversely, deficiencies in the management of FBI records impair the FBI's ability to carry out its essential functions and may result in inquiries and investigations by oversight bodies, as well as adverse public perceptions of the FBI's efficiency, accountability, and management. Records mismanagement can also result in adverse judicial rulings during the discovery process.

1.5. Intended Audience

This policy guide (PG) applies to all FBI personnel. The term "FBI personnel" includes any individual employed by, detailed to, or assigned to the FBI, including members of the armed forces; experts or consultants to the FBI; industrial or commercial contractors, licensees, certificate holders, or grantees of the FBI, including all subcontractors; personal service contractors of the FBI; or any other category or person who acts for, or on behalf of, the FBI, as determined by the FBI Director.

2. Roles and Responsibilities

2.1. Director's Office

2.1.1. The Director

The Director of the FBI:

- Ensures that records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions are created and preserved.
- Has delegated records management authority to the assistant director (AD) of RMD.

2.2. Records Management Division

2.2.1. Assistant Director

The AD of RMD will:

- Serve as the FBI records officer, establishing and overseeing a comprehensive FBI-wide Records Management Program.
- Oversee the management of FBI records throughout their life cycles, including records creation, maintenance and use, and disposition of recorded information in all formats.
- Appoint an FBI-wide vital records officer who oversees the FBI's Vital Records Program, in accordance with the *Vital Records Policy Guide* (0794PG).

2.2.2. RMD Front Office

2.2.2.1. Training Services Unit (TSU)

TSU will:

- Provide records management training and guidance to all FBIHQ divisions, FOs, Legats, groups, and organizations throughout the FBI.
- Ensure all FBIHQ divisions, FOs, and Legats are informed of, and trained in, their responsibilities related to the creation, maintenance, and disposition of FBI records.
- Provide guidance and training to FBI personnel on storing and securing records to reduce the risk of damage and loss of information.
- Provide guidance and training to FBI personnel on saving or mitigating the loss of information in records and restoring original records to a useful condition, if possible.

2.2.3. Records Policy and Administration Section (RPAS)

RPAS will:

- Collaborate with the Records Automation Section (RAS) in the development of records management policies for electronic media.
- Work with the Information and Technology Branch (ITB) and RAS to manage and maintain a policy-compliant records management application (RMA) as part of the FBI's enterprise architecture.
- Establish and disseminate policies and procedures governing the creation, organization, maintenance, use, preservation, disposition, and transfer of all FBI records, regardless of medium or format.
- Conduct periodic FBI records reviews and evaluations to ensure compliance with records management policies and procedures.
- Develop and maintain a network of records liaisons in all FBIHQ divisions, FOs, and Legats, and ensure they receive adequate training to carry out their responsibilities.
- Manage and regularly update the FBI Records Retention Plan and coordinate requests for, and receipt of, all disposition authorities with the National Archives and Records Administration (NARA).
- Manage the storage and maintenance of records.
- Manage the transfer of permanent records to NARA and the destruction of temporary records that have met their retention periods.
- Implement legal holds received from the Office of the General Counsel (OGC).
- Process records modification, permanent charge outs, and expungement requests.
- Conduct and manage FBI-wide record inventories.
- Oversee the storage and maintenance of records in FBIHQ storage areas and advise FBI personnel regarding their records storage and maintenance activities.

2.2.4. Records Automation Section

RAS will:

- Collaborate with RPAS in the development of records management policies for electronic media.
- Provide document conversion services (both imaging and optical character recognition) through the Document Conversion Laboratory (DocLab).
- Conduct electronic recordkeeping certification (ERKC) reviews of all information systems used in the conduct of FBI activities.
- Work with the ITB and RPAS to manage and maintain a policy-compliant RMA as part of the FBI's enterprise architecture.

- Plan and assist with the development, management, and maintenance of the enterprise RMA, in coordination with information technology (IT) divisions, offices, and groups.
- Ensure proper records management requirements are incorporated into the design and deployment of new information and knowledge management systems, which include monitoring system compliance with records management requirements.
- Coordinate and guide the incorporation of electronic recordkeeping (ERK) requirements into IT system development.
- Coordinate and guide the incorporation of recordkeeping requirements into the enterprise RMA file plan as records disposition schedules are updated or added.

2.2.5. Record/Information Dissemination Section (RIDS)

RIDS will:

- Plan, develop, direct, and manage responses to requests for FBI information in accordance with the requirements of the Freedom of Information Act (FOIA) (5 U.S.C. Section [§] 552); the Privacy Act of 1974 (5 U.S.C. § 552a); [FOIA] Executive Order (EO) 13392, *Improving Agency Disclosure of Information*; EO 13526, *Classified National Security Information*; and other applicable Presidential, Attorney General, and FBI policies, procedures, and other mandates, judicial decisions, and Congressional directives.
- Coordinate with OGC's Discovery Coordination and Policy Unit (DCPU) regarding specific FOIA requests.
- Manage the prepublication review program.

2.2.6. National Name Check Program Section (NNCP)

The NNCP will research, analyze, and disseminate information from FBI records, according to the requirements of the NNCP, in order to respond to requests from customer agencies (EO 10450).

2.3. Office of the General Counsel

2.3.1. Employment Law Units

The Employment Law Units will assist with the expungement of information from employee personnel records.

2.3.2. Discovery Coordination and Policy Unit

DCPU will:

- Set the scope, duration, and other characteristics of legal holds.
- Notify FBI personnel of their legal hold obligations.
- Notify FBI personnel of legal hold rescissions.

- Assist FBI personnel with the adjudication and dissemination of record information.

2.4. Information and Technology Branch

The ITB will work with RMD, in coordination with the OGC, to plan and deploy a legally compliant RMA as part of the FBI's enterprise architecture.

2.5. Inspection Division (INSD)

INSD will:

- Monitor records management compliance in FBI FOs, using records review results provided by RMD's RPAS.
- Coordinate with RPAS's Policy, Analysis, and Compliance Unit (PACU) to conduct focused records reviews, as appropriate.

2.6. Criminal Justice Information Services (CJIS) Division

CJIS will send record modifications and expungement requests to the RMD's RPAS.

2.7. All FBIHQ Divisions/Field Offices/Legal Attaché Offices

2.7.1. Assistant Directors, Special Agents in Charge (SAC), Assistant Directors in Charge (ADIC), Chief Division Counsels (CDC), and other Supervisory Personnel

ADs, SACs, ADICs, CDCs, and other supervisory personnel will:

- Appoint records liaisons to assist RMD in the development and implementation of records management policies and procedures.
- Ensure their respective FBIHQ divisions, FOs, and Legats comply with the RMD's policies by creating, approving, and maintaining adequate and proper documentation of all official programs and activities, including properly indexing in Sentinel or other electronic recordkeeping systems when appropriate.
- Provide resources and time to enable FBIHQ division, FO, and Legat personnel to participate in and complete records management requirements and training.
- Appoint FBIHQ division/FO/Legat vital records officers to work with the FBI-wide vital records officer to identify vital records, in accordance with the *Vital Records Policy Guide* (0794PG).

2.7.2. Records Liaison

The records liaison will:

- Represent an FBIHQ division, an FO, or a Legat by coordinating with RMD on all records management policies, procedures, and programs.
- Understand records management concepts and federal records management laws and regulations.

- Review proposed records management policies within an FBIHQ division, an FO, or a Legat, and provide coordinated review responses to the RMD.
- Oversee the creation and maintenance of records in FBIHQ divisions, FOs, or Legats, and advise FBI personnel in their respective divisions, FOs, and Legats on FBI recordkeeping requirements.
- Monitor records destruction and records transfers to ensure compliance, in coordination with RPAS's Records Disposition Unit (RDU), with any legal holds issued by OGC.
- Provide training on records management policies and procedures, in coordination with RMD's TSU.
- Coordinate with RMD to assist with the resolution of issues involving FBIHQ division, FO, and Legat files.
- Oversee continued inventory of paper records.
- Conduct periodic records audits and inventories, in coordination with RPAS.
- Report promptly to the program manager, Records Protection and Recovery Program, about damage to records.
- Report missing hard-copy case files and serials promptly to RPAS's RDU and for classified material, to the division and/or chief security officer (CSO) via the Security Incident Reporting System (SIRS).
- Report missing hard-copy case files and serials that are subject to legal hold promptly to OGC's DCPU. Report missing classified material to the division and/or CSO via SIRS system owners.

Systems owners will coordinate with RAS to ensure the ERKC process is complete and all documentation is accurate and accessible.

2.8. All FBI Personnel

All FBI personnel will:

- Create and maintain adequate, complete, accurate, and proper documentation of FBI programs, investigations, activities, decisions, and transactions.
- Ensure the records they create and/or maintain are filed appropriately in an approved central recordkeeping system, such as Sentinel, and are properly indexed when appropriate.
- Ensure all records made or received while in the FBI's service have been properly recorded or properly and legally disposed of prior to separation from FBI service, in accordance with approved retention schedules.
- Cooperate with FBIHQ division, FO, and Legat records liaisons in the creation, maintenance, and disposition of FBI records.

- Ensure all deletion, destruction, or removal of FBI records complies with policies and procedures established by RMD.
- Comply with legal hold obligations and rescissions.

3. Policies

RMD establishes the requirements, procedures, and policies necessary to ensure FBI personnel manage records effectively to meet the FBI's business needs and to comply with applicable laws and regulations. This PG sets forth those requirements and procedures.

All FBI personnel must comply with the policies and procedures contained in this PG.

4. Procedures and Processes

4.1. Overview

Records management policies and procedures apply to each phase of a record's life cycle:

- Phase 1: Creation and/or receipt (see subsection 4.7.)
- Phase 2: Maintenance and use (see subsection 4.8.)
- Phase 3: Disposition (see subsection 4.9.)

In order to determine what policies and procedures apply to each phase of a record's life cycle, it must first be determined what kind of information is at issue: a record (nontransitory or transitory), a nonrecord, or a personal paper. The *Records Management User Manual* (RM User Manual) provides detailed information and guidance about specific records management procedures to supplement the policies and procedures outlined in this section.

4.2. Definition of a Record

The Federal Records Act of 1950 (see 44 U.S.C. § 3301), as amended, defines records as:

> All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. Records do not include library or museum material made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved for convenience. Recorded information includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

Specific mediums, platforms, and technologies change over time; however, the determination about what constitutes a record remains the same: it is based on content, not form. Communications using advanced electronic tools and media may be records, depending on their content. This PG applies to all records, regardless of physical form or characteristics.

FBI recordkeeping has evolved from paper-intensive records and information management systems to paperless records and electronic information management systems. Today, the FBI's official recordkeeping system is Sentinel, an electronic information management system. All electronic information management systems within the FBI containing records must comply with the policies and procedures governing the management of FBI records.

4.2.1. Questions to Ask in Determining Record Status

A document, regardless of medium, is considered a record if it contains information and is:

- Required to be documented by law, regulation, policy, or an established business practice applicable to the FBI.

- Pertinent to an FBI investigation (including assessments) or intelligence-gathering activities.
- Reasonably necessary to protect the rights of the government or of an individual affected by government action.
- Reasonably necessary to document or explain the basis for a significant action or decision involving the exercise of government authority.
- Needed to conduct government business effectively.
- Necessary to document other significant operations or administrative matters. Examples include changes in the FBI's organizational structure, changes in FBI-wide or FBIHQ division policies, accomplishment of an FBI mission responsibility, an expenditure of funds, a disposition of FBI property, and compliance or noncompliance with a legal obligation.

4.3. Nontransitory Record (Needed for More Than 180 Days)

A nontransitory record is a record needed for more than 180 days that has one or more of the following characteristics: (1) it provides substantive documentation of the FBI's policies and actions, (2) it contains important and/or valuable evidentiary information, and/or (3) it is required to be maintained by law or regulation. A nontransitory record may have a permanent or temporary retention requirement.

A nontransitory record with a permanent retention period is a record appraised by NARA as having sufficient historical or other value to warrant continued preservation beyond the time the record is needed for an agency's administrative, legal, or fiscal purpose. A permanent, nontransitory record will be transferred to, and preserved as part of, the National Archives of the United States after its usefulness to the FBI has ceased. Examples of permanent, nontransitory records include policy files, exceptional case files, and files pertaining to the FBI's "Ten Most Wanted Fugitives." Exceptional case files document the FBI's investigation of significant individuals, events, organizations, precedent-setting programs, unusual investigative methods, and landmark legal cases involving FBI investigations. Additional information about permanent, nontransitory records is available on RDU's Intranet page.

A nontransitory record with a temporary retention period is a record that NARA has determined to be disposable after a specified period of time or after a specific event has occurred. This period may be for one year, or it could span decades. A temporary, nontransitory record has no continuing value after its usefulness to the FBI has ceased.

4.4. Transitory Record (Needed For 180 Days or Less)

A transitory record is a record that has only minimal documentary or evidentiary value and is needed for 180 days or less. Transitory records may include:

- Routine information or publications, working drafts, routine office management documentation, suspense and tickler file notices, and other records that do not serve as the basis for official actions, such as notices of holidays, charitable events, and the like.

- Originating office copies of letters of transmittal that do not add any information already contained in the transmitted material.
- Records documenting routine activities and containing no substantive information, such as routine notifications of meetings, scheduling of work-related trips and visits, and other scheduling-related activities.
- Routine communications, such as reminders of existing policies, work-related guidance, and meeting notices.
- Drafts of, or comments on, proposed policies or actions that are not considered or submitted for consideration by the approving authorities.
- "To-do" lists.

4.5. Nonrecord

A nonrecord is any material that does not meet the statutory definition of a record. As set forth in 44 U.S.C. § 3301, examples of nonrecord materials include:

- Library materials made or acquired and preserved solely for reference or exhibition purposes.
- Stocks of publications or unprocessed blank forms.
- Extra copies of documents preserved only for convenience of reference.

  Note: Not all copies are nonrecord material. Copies of records may be used for different purposes within the FBI, and they may take on record status. For example, copies of other government agency (OGA) records may be maintained by the FBI as records. A nonrecord copy may also become a transitory record or a nontransitory record if substantive notes or comments are added to the document.

4.6. Personal Papers

Personal papers are materials that belong to an individual and are not used to conduct FBI business. They are primarily personal in nature and may be in any format or medium. An example of personal papers includes an employee's copy of his or her Standard Form (SF)-50 ("Notification of Personnel Action"). It is important to note that if a document contains both record and personal information, the document must be treated as a record.

4.7. Records Creation and Receipt (Phase 1: Records Life Cycle)

Under the Federal Records Act, every federal agency is required to make and preserve records containing adequate and proper documentation of its organization, functions, policies, procedures, and essential transactions. See 44 U.S.C. Chapters 29, 31, and 33.

4.7.1. Records Created by the FBI

Every employee, FBIHQ division, FO, and Legat has the responsibility to adequately document activities, decisions, policies, and transactions conducted to further the FBI's mission and to do so according to FBI policies. Documentary materials created in accordance with this responsibility are records.

Only FBI employees may approve official Bureau records. Policy Directive (PD) 0115D, *Approval Authority for Official Bureau Records*, contains additional information.

4.7.2. Supervisory Approval of Administrative Records

FBIHQ divisions, FOs, and Legats are responsible for establishing procedures clearly defining what administrative documents require supervisory approval prior to importing and serializing them to administrative case files. Unless specifically designated, supervisory approval is not required for importing and serializing administrative records. When supervisory approval is required, FBIHQ divisions, FOs, and Legats must establish clearly defined procedures for obtaining required signatures that will not impede the timely serialization of records in the administrative case file.

Supervisors are responsible for making sure staff receives training to ensure documentation requirements are followed. Users are responsible for obtaining supervisory approval of division documents that require such approval and for obtaining this approval prior to importing and serializing them in administrative case files.

The only exemption to this procedure is for documents imported through Sentinel's workflow by those individuals who do not have supervisory functionality. In those instances, when adding administrative documents, the creator can make himself or herself the approver and should do so on those administrative-type documents that the creator's particular office has authorized for self-approval.

4.7.3. Records Received from Non-FBI Personnel or Organizations

Documents, databases, and other information received by the FBI that the FBI must or does take action in the course of its routine duties and responsibilities are FBI records, even though non-FBI personnel or other organizations created them. Examples of these types of records include electronic mail (e-mail) or facsimiles (fax).

An exception to the above is non-FBI-generated, evidentiary material seized by the FBI or its law enforcement partners acquired through court order, warrant, federal grand jury or administrative subpoena or voluntarily provided in the course of an investigation of a particular case or intelligence assessment. This material is treated as evidentiary property and is managed under a different set of rules and regulations than those defined in this PG. Note, however, the "Evidence Chain-of-Custody" (FD-1004) form documents the management of evidence, and it is a record. For more information regarding evidence, see the *Field Evidence Management Policy Guide* (0780PG) and the *Domestic Investigations and Operations Guide* (DIOG) (0667DPG).

4.8. Records Maintenance and Use (Phase 2: Records Life Cycle)

In this phase of a record's life cycle, authentic, reliable, and trustworthy records are readily available (useable) for business purposes and are protected (maintained) from unauthorized alteration, deletion, or destruction.

4.8.1. Records Requirements

Federal regulation Title 36 Code of Federal Regulations (CFR) Chapter XII, Subchapter B, requires agencies to take the following actions in this phase:

- Establish recordkeeping systems for filing records and separating records from nonrecord and personal materials.
- Specify official file locations and storage media for all record types.
- Provide standards, guides, and instructions for easy reference to records.
- Provide reference services to facilitate access to records by authorized users.
- Periodically review and audit recordkeeping systems and practices.

4.8.2. Records Systems

The FBI utilizes many different databases, electronic information systems, and automated records systems to store case or subject data, and each system has its own unique system documentation and distinct records retention requirements. This PG sets forth recordkeeping policies and provides guidance that applies to the content of each system. Questions regarding individual systems should be directed to the responsible system owner. RAS should be contacted for recordkeeping requirements for system content and documentation, as well as ERKC. Additional information is contained in the ERKC Manual.

4.8.3. Central Recordkeeping System–Sentinel

The FBI uses a central recordkeeping system to maintain its investigative, intelligence, personnel, applicant, administrative, and general files. Records are maintained in the central recordkeeping system using a file classification system. Investigative and intelligence documents relating to specific cases, as well as significant administrative documents appropriate for distribution to other divisions and offices, are serialized in relevant case files.

In July 2012, Sentinel became the FBI's official central recordkeeping system. It is a next generation information and case-management system. It has moved the FBI from a primarily paper-based recordkeeping system to an electronic records management system. The Sentinel Intranet site contains guidance about document management within Sentinel.

4.8.4. Indexing Records

Indexing is a fundamental requirement for the management of all types of FBI records, regardless of format, medium, or origin. The FBI must maintain an automated index of subjects, references, victims, and complainants to support FBI investigative and administrative matters. Indexing is mandatory, and FBIHQ divisions, FOs, and Legats must ensure required indexing is accomplished. See DIOG, Section 3 and Appendix J, for additional information.

Within Sentinel, indexing is accomplished by creating an "entity" record. The *Indexing User Manual for Sentinel* contains guidelines that must be followed for entering and searching Sentinel entity records for persons, organizations, or events that are subjects, references, victims, or complainants. It is designed to promote standardized entry and search formats resulting in effective management of the administrative and investigative information collected by the FBI in the performance of its day-to-day activities. RMD's

PACU will conduct monthly reviews to determine the FBI's compliance with the indexing guidance detailed in the manual referenced above.

4.8.4.1. Records Series and Filing Locations

Records are filed according to content and use, regardless of their medium, and are divided into record groups (or series) of files. There are two general types of content: program and administrative.

The majority of the FBI's program or mission-related records are arranged in case files related to a specific file classification. FBI file classifications pertain to federal violations over which the FBI has investigative jurisdiction. File classifications also have been assigned to intelligence, personnel, and administrative matters.

Administrative records facilitate routine organizational or "housekeeping" activities and are created by all FBIHQ divisions, FOs, and Legat offices. Examples of administrative records include time and attendance, travel vouchers, purchase orders, and budget preparation documents. Classifications 319 and 67Q encompass most administrative records; however, some administrative files belong in file classifications such as 242 (Automation) and 261 (Security). For administrative records, file the record copy in the respective division, FO, or Legat subfile designated for the office of origin (OO). See DIOG Appendix J for additional guidance in determining the OO.

With specific approval from RMD's Records Storage and Maintenance Unit, pre-Sentinel Legat classification 319/67Q files may be sent to RMD's Alexandria Records Center (ARC) for storage. RSMU will give special consideration to Legat offices that may experience higher risk for maintaining administrative files. To obtain approval to submit Legat administrative files for storage at the ARC, prepare a lead in Sentinel, addressed to the RSMU, and include an inventory of the files, a total box count, and the desired date of shipment. The *Records Management User Manual* (RM User Manual) contains additional instructions on this topic.

4.8.4.2. File Plan

A file plan is a directory of an office's or a program's records. It outlines the main file headings and subdivision headings for each record series and information system in an office. The plan identifies records in all media, including paper, electronic, and audiovisual, that are physically stored in the office; electronic records, whether on a local or remote computer server or on removable media such as compact discs (CD); records on other nonpaper media, such as digital video discs (DVD), audiotapes, and film; and records stored in other office file storage areas. When records are organized in accordance with a file plan, it is easy to periodically move inactive and noncurrent files out of an office area to other storage locations, freeing up needed office and computer space. Section 3 of the RM User Manual contains detailed guidance about file plans, as well as a sample file plan.

The point when files change from pending to closed or inactive is referred to as a file cutoff. File cutoffs identify and control records in manageable blocks, usually organized by fiscal or calendar year. Some files do not have event-driven cutoffs. These files are

identified and cut off based on their retention. Section 4 of the RM User Manual contains detailed guidance about file cutoffs and their implementation.

4.8.5. Case Management

FBI personnel must create and maintain authentic and reliable records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14 and DIOG Appendix J. Consult Section 5 of the RM User Manual for procedural information and records management guidance for:

- Case files.
- File jackets.
- File types.
- Universal Case File Numbers.
- Serializing.
- Subfiles and subfile designators.
- 1A (FD-340) envelopes.
- Compressed files.
- File consolidation.
- Dual-captioned cases.
- Cover sheets and media labels.
- Records managed by the Executive Secretariat (EXEC SEC).

Procedures for subfiles and subfile designators are set forth in subsection 5.6. of the RM User Manual. ITB and FBI personnel must make sure only dashes, alpha, numeric, and/or blank entries are allowed in the subfile name field of case files.

The use of compressed files is no longer authorized. Compressed files were small paper case files (normally one to ten serials in scope) that were opened in the same file classification and placed together in a single file jacket in order to conserve shelving space. See subsection 5.8. of the RM User Manual for additional information.

4.8.6. Managing Administrative Records

Classifications 319 and 67Q are designated for administrative and personnel-related records. A subfile has been opened for each FBIHQ division, FO and Legat for each of the 319 and 67Q categories. However, not all FOs will need to use all the established case file numbers. Administrative records should be filed under the classification 319 categories rather than under an investigative or an intelligence classification.

It is not necessary to import each 319 and 67Q document. If a document needs to go through the Sentinel workflow approval process, it should be imported into the appropriate 319 or 67Q file within Sentinel. If the document does not need to go through the Sentinel workflow approval process (e.g., time and attendance records or a

supervisor's drop files), it does not need to be imported into Sentinel. It may be maintained in a shared drive or a paper folder for the applicable retention period. The disposition of 319 and 67Q matters is discussed in subsection 4.9.11. of this PG.

Performance appraisal reports (PAR) must continue to be maintained in paper format with their original signatures. PARs are maintained by the RMD at the ARC.

Section 6 of the RM User Manual contains additional guidance.

4.8.7. Storing Paper Records

FBI paper records are stored in FBIHQ divisions, the ARC, FOs, off-site locations, and Legats around the world. All locations are required by 36 CFR §§ 1223-1238 to meet minimum standards to properly store and protect federal records. Section 8 of the RM User Manual contains detailed guidance regarding records storage.

4.8.7.1. Files at FBI Headquarters

The RMD's Records Storage and Maintenance Unit (RSMU) is responsible for overseeing the storage and maintenance of records in FBIHQ storage areas and advising FBI personnel concerning records storage and maintenance activities. The ARC is the main facility for storage and maintenance of (1) FBIHQ closed and pending case files, (2) Legat closed files, (3) closed files from inventoried FOs, (4) security and medical subfile of active personnel, and (5) micrographics, all with a classification of SECRET or lower. FBIHQ paper records with a classification higher than SECRET or containing Sensitive Compartmented Information (SCI) or other matters requiring restricted access are stored at FBIHQ in the Special File Room, J. Edgar Hoover Building [redacted] b7

4.8.7.2. Files at Legal Attaché

A Legat maintains its pending files. The Security Division's (SecD) Legat Support Program ensures Legats are in compliance with FBI, Department of State, and other national requirements pertaining to secure areas, closed storage of classified information up to the SECRET collateral level, and, where applicable, areas accredited as Sensitive Compartmented Information Facilities (SCIF). Most closed Legat files are stored at the ARC. Subsection 9.3. of the RM User Manual contains detailed procedures for shipping records to the ARC.

4.8.7.3. Files at a Field Office or a Resident Agency (RA)

The FO headquarters city maintains the FO's pending files. The relevant RA location may maintain its unclassified and classified materials if it is in compliance with the requirements for classified material storage. Detailed guidance regarding classified material storage can be found in the *Safeguarding Classified National Security Information Directive and Policy Guide* (0632DPG).

4.8.7.4. Secure Storage Location Requirements

SecD is responsible for determining the requirements for all storage locations. The "Open Storage Secure Area Checklist" is a checklist of secure area facility requirements guidelines.

4.8.7.5. Environmental Storage Policy

All records, regardless of format or medium, must be stored in accordance with 36 CFR Part 1234, which sets forth environmental standards and preservation requirements. Section 8 of the RM User Manual contains detailed guidance regarding the minimum requirements for environmental storage of federal records.

4.8.8. Transferring Records

Detailed guidance on how to transfer records is included in Section 9 of the RM User Manual.

4.8.9. Retrieving Records

FBI employees and authorized personnel may request access to stored, paper files. Case files maintained electronically in the FBI's central recordkeeping system (Sentinel) must not be duplicated in paper and filed. Section 10 of the RM User Manual contains detailed guidance about paper records retrieval.

4.8.9.1. File-Automated Control System

The File Automated Control System (FACS) was a library system that was used to track the checking out, and returning of, all FBIHQ paper files (investigative, administrative, and personnel). As of fall 2014, FACS is no longer in use.

Subsection 10.1. of the RM User Manual contains additional information about this system.

4.8.9.2. File Request Automation Project (FRAP)

FRAP is an electronic system used to request (1) paper files (investigative, administrative, and personnel), (2) closed FO files sent to the ARC for storage as part of RMD's Field Office Inventory Project, and (3) Legat files stored at the ARC. This system has been constructed using SharePoint and InfoPath and is deployed on FBINet (the FBI [classified] Network). Files may be accessed through the FRAP Intranet site by following the instructions for ordering a file. The file is then checked out and either physically or electronically sent to the requester. When physically sent, a copy of the FRAP request form will be attached to the file for easy identification. The FRAP request form must be kept attached to the file.

The FRAP User Guide contains step-by-step guidance and additional information about this system.

4.8.9.3. Maintaining Custody of Files

An individual who checks out a file is responsible for the file until it is returned to the RSMU. In order to maintain security and access control over the information contained within the file, the individual must not give or lend the requested file to other FBI personnel. The file must be returned to RSMU and a new request must be completed.

4.8.9.4. Returning Files

All files must be returned to the RSMU within 90 days of receipt unless the requester requires additional time. To retain a file longer than 90 days, the requester must seek an

extension through FRAP. The FRAP request form must be attached to the file when a file ordered through FRAP is returned.

4.8.10. Retrieving Information from Records

4.8.10.1. Outside the FBI

4.8.10.1.1. Freedom of Information and Privacy Acts (FOIPA)

FBI records can be requested through FOIPA. The Policy Directive (PD) 0481D, *Freedom of Information Act and Privacy Act Requests* establishes actions to be taken by FBIHQ divisions, FOs, and Legats when asked by the RMD for assistance in responding to records requests.

4.8.10.1.2. National Name Check Program

The NNCP disseminates information from FBI files in response to name check requests received from federal agencies and other law enforcement entities, including internal FBI offices; components of the legislative, judicial, and executive branches; and intelligence agencies. The NNCP also conducts name check requests of those persons within arms-reach of the President.

4.8.10.1.3. Mandatory Declassification Review

Mandatory declassification reviews of FBI material are generally requested by NARA, Presidential libraries, and the public. The *Declassification of Classified National Security Information Directive and Policy Guide* (0623DPG) sets forth the policies and procedures for carrying out the declassification requirements articulated in EO 13526.

4.8.10.1.4. Legal Holds

FBI personnel have an obligation to ensure all records and nonrecords relevant to a pending litigation or reasonably anticipated matter in litigation (or other proceeding, including criminal investigations, prosecutions, and appeals) and other inquiries, investigations, and inspections are identified and protected from destruction or deletion, even as an exception to standard records disposition practices and schedules, until all legal and official uses are concluded and personnel receive written confirmation from OGC when the identification and protection of such information is no longer necessary. Identifying such records and marking them for retention is referred to as a "freeze" or "legal hold." Whenever legal holds are initiated, all regularly scheduled destruction and/or transfer activities are suspended until OGC has notified FBI personnel that the legal hold has been rescinded. The *Legal Hold Policy* (0619D) contains further information concerning when legal holds may be issued and the roles and responsibilities of FBI personnel and others with regard to a legal hold.

4.8.10.1.5. Assistance to Other Agencies

If FBI documents and information are to be disseminated to other domestic and foreign agencies for use in investigative and intelligence programs, the documentation and records retention requirements for this type of dissemination are contained in DIOG subsections 12.6. and 12.7.

4.8.10.2. Personnel Records

4.8.10.2.1. Electronic Official Personnel Folder (eOPF)

The FBI's official personnel folders (OPF) are available online for FBI employee access via the eOPF application. Access is only available on a UNet (unclassified network) computer with an FBI Internet Protocol (IP) address.

The eOPF provides electronic, Web-enabled access for all federal agency employees to view and manage employment documents. All employees are able to view their own OPFs through the eOPF application. It also includes security measures that ensure the integrity of the system and employee documents in the system. For more information on accessing an eOPF, see the Human Resources Division's eOPF Information Intranet site.

4.8.10.2.2. Paper Personnel Records

Personnel records include the applicant case file; the OPFs of agent personnel retired or separated prior to August 2012 and professional staff personnel separated less than five years prior to January 2012; the security (S) and medical (M) subfiles of active personnel; financial subfile (Sub-F); and PARs. Previously, personnel records included the other government service subfile (Sub-OGS); however, the sub-OGS is no longer maintained as a separate subfiles, it has been incorporated in the eOPF. FBI personnel may submit a formal request for copies of their personnel records. The procedure to do this is set forth in subsection 7.2. of the RM User Manual.

4.8.11. Electronic Recordkeeping Certification (ERKC) Program

An electronic information system or a knowledge management (KM) system (collectively, system) contains and provides access to computerized FBI records and other information. A system containing records must comply with the policies and procedures governing the management of FBI records. The RMD AD, as the FBI records officer, has the authority to approve, or withhold approval of, any system in use or under development.

The FBI records officer has delegated the review of systems to RMD's Records Management Application Unit (RMAU). No system may be utilized to conduct FBI business and house FBI records without review by the RMAU and final certification by the FBI records officer.

The goal of the ERKC process is to ensure systems comply with recordkeeping requirements, including the proper creation, maintenance, use, and disposition of FBI records. The ERKC process evaluates system compliance with records management criteria. The process is designed to guide systems owners and developers with assessing and incorporating records management criteria into system requirements specifications and ensuring fulfillment through review of documented test results. The ERKC process consists of identifying systems containing records; helping system owners, project managers, and developers understand ERK criteria; ensuring system requirements specifications satisfy ERK criteria; and validating ERK functionality through review of system test results.

The FBI's ERKC Manual defines the authorities, roles, responsibilities, processes, and documentation requirements that govern the certification of FBI-owned and FBI-sponsored IT systems and serves as a guide for system developers, system owners, project managers, and certification team members concerning the activities required for an FBI-owned or FBI-sponsored system to achieve ERKC.

4.8.12. Metadata

Metadata is defined as data describing information—in particular, its context, content (including author), structure, and its management through time. It is critical that metadata used is detailed and descriptive to effectively manage electronic records throughout their life cycles.

Metadata requirements for recordkeeping purposes are jointly established by both the originating program office and by RMD. With adequate metadata, records are retrieved effectively and purged when no longer needed, without having to be printed for records disposition purposes. Policy for incorporating metadata tags into electronically stored information is located in PD 0249D, *Metadata Tagging of Electronically Stored Information in FBI Systems*, and the ERKC Manual, Appendix B.

4.8.13. Data Backup Retention

The FBI routinely maintains data backups on computer drives or computer media to protect data from system and server failure or from data corruption. All FBI electronic information systems must be backed up to ensure the authenticity, reliability, and integrity of the information within the systems. A full-data backup of each FBI electronic information system is retained until superseded by the next full-data backup, except for FBINet file/print servers (SECRET enclave). For these, a full-data backup is retained for 90 calendar days. See PD 0076, *Data Backup Retention*, for additional information on this matter.

Legal holds or other special inquiries are the only exceptions to this data backup retention policy. In these instances, backups must be maintained until OGC rescinds the legal hold or other preservation request.

The approved retention period for data backup is formulated as General Records Schedule (GRS) 20, "Electronic Records," Item 8, as specified by NARA, 44 U.S.C. § 3303a(d). The approved retention period for system backups is formulated as GRS 24, "Information Technology Operations and Management Records," Item 4a, as specified by NARA, 44 U.S.C. § 3303a(d). The backup retention plans for mission specific electronic systems are evaluated as part of the development of records retention guidance for the specific system.

IT systems administrators must maintain data backups in accordance with this PG. OGC is responsible for notifying IT systems administrators when there is a need to retain electronic information beyond the standard retention period for a given electronic information system and for notifying the IT administrators when an exception to the approved retention period has expired.

4.8.14. Capturing and Preserving Electronic Records

All FBI personnel bear responsibility for identifying, capturing, and moving electronic records into a recordkeeping system. To ensure proper preservation, personnel must import electronic communications that are nontransitory records into an ERK system such as Sentinel.

Whenever possible, personnel should import electronic communications in the format in which they were generated, otherwise known as "native format." If an electronic communication cannot be imported in its native format (such as a voice message), it should be preserved in another format (e.g., FD-302 or electronic communication [EC]) in the appropriate recordkeeping system, such as Sentinel.

4.8.14.1.1. Deletion of Electronic Copies

Copies of documents are often maintained in electronic form, across all enclaves, either on office shared drives, individual workstations, or portable magnetic or optical media (e.g., flash drives, CDs, diskettes, or tapes). Many of these copies are word processing documents and are kept for convenience of reference or reproduction. If these copies are created solely to produce a convenience copy, once it is verified the record is appropriately filed, they should be deleted, unless subject to a legal hold. It is each employee's responsibility to manage these copies on any FBI information system he or she uses.

4.8.15. Electronic Mail

E-mail is a frequent means of communication within the FBI, and the information contained in e-mails must be managed accordingly. FBI personnel are responsible for managing the e-mails they send and receive.

FBI personnel with access to the FBI's e-mail systems must determine the record status of e-mails sent from, or received in, their e-mail account(s). An e-mail may be a nontransitory record (needed for more than 180 days), transitory record (needed for 180 days or less) or nonrecord. When doubt exists about whether or not an e-mail is a nontransitory record e-mail, it should be treated as a nontransitory record e-mail and imported into Sentinel or a successor central recordkeeping system.

E-mails (whether record or nonrecord) that are responsive to legal holds, investigations, FOIPA requests, or special inquiries of any kind must be preserved. PD 0619D, *Legal Hold Policy*, contains further information.

4.8.15.1. UNet E-Mail

Communications received via UNet that contain record material must be uploaded to FBINet to ensure proper records management. UNet e-mails should be copied to FBINet and imported into Sentinel to the relevant FBI case file.

To import these unclassified e-mails into Sentinel, use the "UNet to FBINet File Transfer System" (UNet "Uplift") to transfer the e-mail to FBINet, where it can be filed into Sentinel. See the RM User Manual for further instructions on using Uplift.

4.8.16. Nontransitory Record E-mails (Needed for More Than 180 Days)

A nontransitory record e-mail is a record needed for more than 180 days that provides substantive documentation of the FBI's policies and/or actions, contains important and/or valuable evidentiary information, or is required to be maintained by law or regulation. The principal categories of materials to be preserved are records that:

- Document the formulation and/or execution of policies and decisions and the taking of necessary actions.
- Facilitate action by FBI officials and their successors in office.
- Permit Congress or other duly authorized agencies of the government to conduct a proper scrutiny of the FBI.
- Protect the financial, legal, and other rights of the government and of persons directly affected by the government's actions.

Examples include e-mails that document:

- An investigation or an intelligence analysis. Examples of e-mails that fall into this category include:
  - Exchanges between special agents (SA) or OGA personnel discussing case issues.
  - Electronic surveillance (ELSUR) requests.
  - Requests for assistance from other parties.
  - Surveillance reports.
  - Intraoffice records requests and responses that pertain to an investigation or an analysis.
  - Pertinent intelligence analyses received from another agency.
  - Task force requests for additional funding.
- Significant decisions reached at meetings, conferences, or through e-mail exchanges, such as executive decisions creating or modifying an FBI policy.
- Official agreements with entities outside the FBI.
- Quotes from vendors in response to requests for pricing proposals, which are subsequently used as the basis for contract agreements.
- FBI reorganizations.
- On-duty injuries requiring hospitalization.
- Formal assignments of divisional, FO, and Legat roles and responsibilities.
- End of the fiscal year final reports of expenditures, procurement of goods and services, and annual accountability by all FBI personnel for equipment issued to them.

4.8.17. Filing Nontransitory Record E-Mails in Sentinel

FBI personnel must use the Record Marking Tool (RMT) to import nontransitory record e-mails into the appropriate case file in Sentinel. Subsection 12.1. of the RM User Manual contains additional information about the RMT.

Systems such as Microsoft Outlook, Law Enforcement Online (LEO) mail, and UNet mail are communication systems, not electronic recordkeeping systems. To ensure the retention of nontransitory record e-mails in Sentinel, message creators, recipients, or professional staff personnel must complete the steps necessary to scan and import e-mails into Sentinel or a successor central recordkeeping system. Copies of nontransitory record e-mails must be added to the appropriate case file(s) before the original online e-mail message can be deleted. Attachments, as well as transmission and receipt data about the e-mail, must also be saved as part of the record. Transmission and receipt data include the sender's name, date, subject, recipient(s), and any requested return receipts. See Section 12 of the RM User Manual for instructions.

FBI personnel may not create or send a record (transitory or nontransitory) using nonofficial electronic messaging accounts unless the FBI personnel (1) copy their official electronic messaging accounts in the original creation or transmission of the records, or (2) forward complete copies of the records to their official electronic messaging accounts no later than 20 days after the original creation or transmission of the records.

For nontransitory record e-mails, FBI personnel must also complete the steps necessary to import the e-mail into Sentinel:

If the nontransitory record e-mail does not relate to a specific FBI case, the e-mail message should be filed in the related classification zero (0) file, which serves as a holding file for unsubstantiated allegations. For example, if the e-mail message provides general commentary or guidance on bank robbery matters, but does not contain information related to an actual or specific investigation, the message should be filed in the 91-0 file. If a specific case is later opened or identified, the e-mail message can be transferred from the zero (0) file to the relevant case file.

4.8.18. Transitory Record E-Mails (Needed for 180 Days or Less)

Transitory record e-mails are e-mails of short-term interest (180 days or less) and have minimal documentary or evidentiary value to the FBI. As is the case with nonrecord e-mails (discussed below), transitory record e-mails should not be preserved in an FBI recordkeeping system. Absent a legal hold, when no longer needed, these e-mails should be deleted by the creator/receiver. Examples of transitory record e-mails include:

- Routine requests for information or publications, such as e-mails sent to the Office of Public Affairs requesting copies of the "Ten Most Wanted Fugitives" poster and copies of replies.
- Quasi-official notices, such as announcements of upcoming events from the sending office. For example, transit subsidy requirements and forms and annual holiday party guidance are transitory records of the sending office.

- Documentation of routine activities, such as meeting notifications, reminders of midyear performance plan reviews, and unit award nominations sent to a division's or an FO's front office.
- Working drafts of proposed policies or documents.
- Routine requests for supplies and similar office management documentation.
- Suspense files and "to-do" lists.
- Confirmation of training registration, conference attendance, or travel plans.
- Messages sent enterprisewide, such as holiday closing notices or Combined Federal Campaign information. While senders may have an obligation to retain messages for a short time, recipients may delete them when no longer needed.

4.8.19. Nonrecord E-Mails

A nonrecord e-mail contains information that does not meet the definition of a federal record. A nonrecord e-mail has no documentary or evidentiary value to the business of the FBI and does not require retention beyond its useful life, as determined by the creator and/or recipient, unless subject to an external request or legal hold, as discussed above. Examples of nonrecord e-mails commonly include e-mails that transmit:

- Copies of records, such as ECs already serialized in Sentinel.
- Copies of FBI publications, such as the DIOG, *The Investigator*, or the *Law Enforcement Bulletin*.
- Informal notes and cover notes that are merely informative in nature and do not include content otherwise warranting preservation as records.
- Copies of PowerPoint training slides from FBI-provided courses.
- Electronic versions of blank forms such as the FD-772, "Report of Foreign Travel."
- Copies of notices received by individuals, such as announcements of upcoming blood drives, seminars, Combined Federal Campaign fundraisers, and similar events.
- FBI personnel anniversary, retirement, and other announcements.
- Discussions between personnel about lunch or other non-work-related activities.
- Other notifications of a personal nature.

FBI personnel with access to the FBI's e-mail systems must determine the record status of e-mails sent from, or received in, their e-mail account(s). Across all enclaves, absent a legal hold, nonrecord e-mails should be deleted from all FBI-managed e-mail systems when no longer needed. Care should be taken by FBI personnel not to comingle record and nonrecord information in e-mails. This ensures nonrecord information is not accidentally transferred or retained in any FBI record repository or system.

4.8.20. Intranet Sites

The Federal Records Act applies to all federal agency records, including Intranet-based records (e.g., records created on SharePoint sites). The E-Government Act of 2002 (Public Law 107-347) places a number of public site requirements on the Office of Management and Budget (OMB), NARA, and agencies in the areas of enterprise architecture, information access and security, and accessibility to persons with disabilities.

FBI personnel who use electronic communication venues to reach agreements or to transmit messages on substantive matters relating to FBI activities, including investigative and intelligence activities, must treat the exchange as a nontransitory record. The nontransitory record must be entered into Sentinel or a successor central recordkeeping system.

Many FBI Intranet pages contain organizational charts, publications, graphic presentations, interactive programs, and links to information repositories. RDU, in conjunction with the Information Technology Infrastructure Division (ITID), has developed a disposition authority, N1-065-04-6, for the administrative records associated with the FBI's public Web site, www.fbi.gov. RMAU, in conjunction with RDU, also assists program offices with developing disposition authorities for records maintained on internal and external FBI sites.

4.8.21. Electronic Information Sharing Technologies

The FBI encourages the participation of FBI personnel in both internal FBI-sponsored and external United States government (USG)-sponsored electronic information-sharing technologies (EIST) and the use of EIST.

Information exchanged through EIST may constitute record material, even though the EIST may not be an approved FBI recordkeeping system. All information that meets the definition of a federal record, including data and metadata created or received using EIST, must be entered into an authorized FBI recordkeeping system. Records management procedures for FBI-sponsored EIST must be developed in collaboration with RMD and are subject to RMD's approval. RMD's approval must be obtained before FBI personnel establish, configure, and/or operate EIST. See *Social Media and Other Electronic Information Sharing Technologies Directive and Policy Guide* (0579DPG) for additional information.

4.8.22. Imaged Records and Standards for Scanned Documents

Both paper and electronic versions must be managed according to RMD's guidance. See the RM User Manual; PD 0774D, *Records Management Standards for Scanned Documents*; and PD 0671D, *Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format*, for additional guidance.

Divisions considering the destruction of paper records after conversion to digital images must have authorization to do so from RMD.

4.8.23. Standards for Photographic Records

Photographic records and negatives may have a permanent retention, and many will be maintained for long retention periods. When practical and possible, FBI electronic photographic records that originated in digital format created by using medium- to high-quality resolution settings appropriate for continued preservation must be produced and retained in a manner appropriate to meet recordkeeping standards and requirements. RMD should be consulted for guidance on the standards for the creation, maintenance, and disposition of digital photographic records.

Digital photographic records and negatives generated by the FBI that are evidentiary or documentary in nature and considered FBI records, such as crime scene photographs, must be filed in the related investigative case file and will assume the retention period established for the file.

The *Field Evidence Management Policy Guide* (0780PG) and the DIOG set forth additional guidance regarding the storage and disposition of evidence, as well as the accompanying recordkeeping requirements.

4.8.24. Restrictions on FBI Records

Certain types of information must be protected from disclosure. Three examples are discussed briefly below. This is not an all-inclusive list; specific statutes may impose additional burdens on disclosures. For more guidance, see DIOG Sections 14 and 18.

4.8.24.1. Sensitive and Restricted Information

FBI personnel are required to comply with statutory, regulatory, and FBI policy requirements for the protection of certain sensitive and restricted information. Guidance on the application of national security classifications, caveats, and compartmented access requirements is located on the SecD Intranet site.

4.8.24.1.1. TOP SECRET (TS) Information /Sensitive Compartmented Information

TS/SCI must not be serialized into Sentinel. However, a placeholder, documenting the existence and attributes of the TS/SCI material, must be created and serialized into Sentinel. For details on the serialization of TS/SCI material, please see the following document, which is posted on the "One-Shots" library on the RMD Intranet site.

4.8.24.2. Federal Grand Jury Material

Federal Rules of Criminal Procedure 6(e) generally prohibits disclosing "matters occurring before the grand jury." DIOG subsection 18.6.5. sets forth policies and guidance regarding the receipt, use, disclosure, and storage of grand jury material.

4.8.24.3. Federal Tax Information

FBI personnel must protect information contained in tax returns from disclosure. SecD's FTI program manages policy, training, oversight, and coordination of FBIHQ-level efforts and programs with regard to FTI, in accordance with laws and policies and with direction from the Internal Revenue Service (IRS) and the Department of Justice (DOJ).

DIOG Appendix N sets out guidance on the acquiring, handling, storing, and disposition of FTI.

4.9. Records Disposition (Phase 3: Records Life Cycle)

RMD is the sole authority for the disposition of FBI records, regardless of location or medium. "Disposition" is a comprehensive term referring to either the permanent transfer of nontransitory records to NARA or the destruction of all other records.

4.9.1. Modification and Destruction of Records

RMD is the sole entity with authority to destroy or delete FBI records and is the sole entity that can authorize the destruction or deletion of FBI records. RMD (or its designee) will modify or destroy records, as authorized or required by law and in accordance with approved retention schedules. RMD is also the sole entity with authority to modify or destroy electronic references or pointers in nonrecord automated systems (i.e., Automated Case Support [ACS]), which serve to point the user to the FBI's electronic records systems.

All FBIHQ divisions, FOs and Legats must advise RMD of the need to modify or destroy records. In Sentinel, this can be accomplished by setting a lead to DK-RPAS (RMD Records Policy and Administration Section) and requesting a permanent charge-out (PCO) of the relevant material

4.9.2. Records Retention Plan

RDU implements and updates the FBI Records Retention Plan, which governs the retention, disposition, and transfer of all FBI records, regardless of location or format. The FBI Records Retention Plan refers collectively to the GRS as well as the individual disposition schedules (SF-115 "Request for Records Disposition Authority") the FBI submits to NARA for approval.

Disposition schedules are broken down by records series (i.e., file classification) or by system name. For each records series or system, the disposition schedule includes a brief description of the records, a breakdown of the types of records covered by the records series or system, and disposition instructions for each.

4.9.3. Purpose of Record Retention Plan

The FBI Records Retention Plan:

- Ensures compliance with the law. Federal agencies are required to have retention schedules for their records, regardless of format.
- Reduces the risk that records will be disposed of before they have met their authorized retention periods.
- Ensures records are retained as long as needed for business purposes and disposed of when no longer needed.
- Facilitates discovery during litigation.
- Protects the FBI from litigation resulting from the destruction of unscheduled records.

- Frees up costly office and computer space, removing records no longer needed for current business activities.

4.9.4. Records Not Included in the Records Retention Plan

Records that are not included in the FBI Records Retention Plan or the GRSs are not authorized for disposition. These records must be retained; they cannot be deleted or destroyed. Owners and creators of these records should contact RDU for assistance with hard copy paper records and RMAU for assistance with electronic records.

4.9.4.1. Creating a New Series of Records

FBI personnel must contact RDU (paper records) or RMAU (electronic records) if the program, FBIHQ division, FO, or Legat begins creating a new series of records, obtains authorization for a new file classification, creates a new electronic information system, or substantially changes the ways in which records are created and used. RDU and RMAU will work with FBI personnel to analyze retention requirements and develop a retention schedule.

4.9.5. Applying the Records Retention Plan

The FBI Records Retention Plan sets forth specific instructions about the length of time records must be maintained. Section 13 of the RM User Manual contains detailed guidance regarding the disposition of records. The RM User Manual supplements the general policy discussion below and should be consulted as a reference tool. Note: Legal holds supersede any destruction guidance provided in the RM User Manual until such holds have been lifted.

4.9.6. Preservation of Nontransitory Records with Permanent Retention

The FBI Records Retention Plan designates a small percentage of all FBI records for permanent retention and allows for the destruction of the remainder. "Permanent retention" means a file will never be deleted or destroyed. The file will be processed by RDU and transferred to NARA for continuing retention after a specified number of years following the closing of the case. When an electronic case file is transferred to NARA, it will be deleted from the FBI's electronic system by RDU. NARA will make the file available for researchers studying the FBI's investigations and activities, when appropriate. See Section 13 of the RM User Manual for additional guidance.

4.9.7. Disposition of Nontransitory Records with Temporary Retention

Temporary records are records deemed by NARA to have no continuing value after their usefulness to the agency has ceased. These records are not transferred to NARA for preservation, but rather are destroyed either after a fixed period or after a specific event has occurred. Their retention periods may range from months to years. Temporary records are disposed of in accordance with a NARA-approved records schedule, unless those records are subject to a legal hold. RMD is the sole entity with authority to destroy or delete FBI records and the sole entity that can authorize the destruction or deletion of the FBI's temporary records.

4.9.8. Disposition of Transitory Records

Transitory records do not need to be scanned or imported into Sentinel. They may be deleted by the user/receiver when no longer needed or deleted according to an automated deletion process, unless those records are subject to a legal hold.

4.9.9. Disposition of Investigative and Intelligence Records

RDU (paper records) and RMAU (electronic records) directly manage the disposition of all investigative and intelligence-related records. This ensures that the complex disposition requirements for these records are accurately and consistently applied. Because most of the mission-related activities of the FBI are documented in investigative and intelligence classifications, offices must retain these case files until RDU or RMAU issues specific disposition instructions or directs the transfer of records to FBIHQ for processing. Offices must not initiate disposition actions without prior guidance from RDU or RMAU.

4.9.10. Disposition of Records Pertaining to Evidence

Once a case is closed and all investigative needs have been exhausted, non-FBI-generated evidence is returned to the owner/contributor, destroyed, or forfeited. FBI-generated evidentiary and nonevidentiary items, regardless of size, that are documentary in nature and considered FBI records, such as chain of custody forms, agents' notes, crime scene photographs, and laboratory analyses, should be filed in the related investigative case file and will assume the retention period established for the file, unless modified by a legal hold.

The *Field Evidence Management Policy Guide* (0780PG) sets forth the policy regarding the storage and disposition of evidence, as well as the accompanying recordkeeping requirements.

4.9.11. Disposition of Administrative Records: Classifications 319 and 67Q

All classification 319 and 67Q records must be maintained in Sentinel or in a successor central recordkeeping system.

Most of the FBI's administrative records are temporary records and may be destroyed after their retention periods have expired. This means after a certain period has lapsed, the records can be destroyed with the approval or at the direction of RDU (paper records) or RMAU (electronic records), unless these records are subject to a legal hold. Once the retention period has expired, and authorization has been obtained, eligible classification 319 and 67Q paper serials can be destroyed.

4.9.12. Disposition of Personnel-Related Records

Personnel subfiles are maintained at the ARC, regardless of the location of the FBI personnel. The disposition of subfiles Sub-M, Sub-S, and Sub-F, is determined by the "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration and Addendums 1, 2, and 3" and the FBI Records Retention Plan.

RDU applies disposition to unsuccessful applicant records in accordance with retention schedules, unless they are subject to a legal hold.

4.9.13. Disposition of Draft Documents

Working files, such as preliminary drafts, notes, and other similar materials, are to be destroyed when the final documents have been approved by the FBI official with authority to do so, unless they:

- Are subject to a legal hold.
- Relate to pending FOIPA requests.
- Contain unique information, such as substantive annotations or comments that add to a proper understanding of the FBI's formulation and execution of basic policies, decisions, actions, or responsibilities and were circulated or made available for approval, comment, action, recommendation, follow-up, or to communicate FBI business.
- Have some other business reason requiring retention for reference purposes.

This guidance applies to all drafts created in any medium.

4.9.14. Disposition of Personal Files

Personal papers are not federal records and are not imported, serialized, indexed, or filed in FBI records management systems. They should be maintained separately from office records and may be disposed of at the owner's discretion, unless subject to a legal hold or FOIA.

4.9.15. Disposition of Nonrecord Materials

Nonrecord material does not need an authorized disposition. It is destroyed when FBI personnel or the responsible office no longer needs it or when the information has served its intended purpose, unless subject to a legal hold or FOIA. As a matter of good recordkeeping practice, FBI personnel should file nonrecord materials separately from records. FBI personnel should review nonrecord materials annually, and materials that are no longer useful should be destroyed.

4.10. Orphaned Records

Orphaned records are records left behind by the creators or owners. Orphaned records are sometimes abandoned in offices after personnel have moved or a reorganization has occurred. FBI personnel should be aware of their responsibilities in ensuring records in their custody are not inadvertently left behind during office moves. Similarly, supervisors should ensure that departing FBI personnel manage records in their possession prior to departure. Anyone finding orphaned records should contact the RMD Help Desk, and RMD will help determine the disposition of those records. See subsection 13.13. of the RM User Manual for additional guidance.

4.11. Reporting Missing Files and Serials

Files or serials missing for 30 calendar days or longer must be reported by the records liaison, via EC, to the RDU within 30 calendar days of discovery. Reasonable efforts to locate missing files or serials must be undertaken, and the status of those efforts must be reported to the RDU every 60 days after the initial report is filed. RDU shall report any missing files or serials to NARA that have not been located within six months of the date of the reported loss.

4.11.1. Reporting Missing Files and Serials Subject to Legal Hold

If missing files or serials contain documents subject to a legal hold, OGC's DCPU must be notified immediately.

If missing files or serials contain classified material, this must be reported immediately to the division and/or CSO, who will then report it to the Security Compliance Unit at FBIHQ, as directed by PD 0610D, *Security Incident Program*.

If missing files or serials can be recreated from other sources, the file should be recreated, and the new file must reference that fact. In addition, if a missing file or a serial is recreated from other sources, and the materials are subject to a legal hold, the FBIHQ division or FO must notify DCPU immediately.

The records liaison must contact RDU if, after reporting a missing file or serial, the material is subsequently located.

4.12. Expungement of FBI Records

4.12.1. Court-Ordered Expungements

RMD's RPAS is responsible for processing court-ordered requests for the expungement of FBI case files. RPAS does this in accordance with PD 0169D, *Expungement of FBI Records*.

RPAS only processes expungement requests received directly from the CJIS Division or from OGC. Should an FBIHQ division or an FO receive an expungement request from a local, state, or federal court, the expungement request must be forwarded to the CJIS Division's Criminal History and Investigative Service Unit for processing.

4.12.2. Privacy Act Expungements

The Privacy Act allows individuals to request expungement of their records. For example, an individual may ask that erroneous information contained in his or her FBI records be expunged. All Privacy Act expungement requests are referred to the RMD's Record/Information Dissemination Section for processing.

4.13. Unauthorized Destruction of FBI Records

All FBI personnel are responsible for preventing the unauthorized destruction, damage, or alienation (removal from FBI custody) of records. The unlawful removal, defacing, alteration, or destruction of federal records may result in penalties, including fines and imprisonment. If files or serials are missing or destroyed due to negligent or willful

misconduct of FBI personnel, the Office of Professional Responsibility (OPR), OGC, and RDU must be notified immediately.

RDU must then report the unauthorized destruction of any files or serials to NARA.

4.14. Damage to FBI Records

FBI records can be damaged by natural or manmade events or causes. The extent of damage can vary from minimal to extensive and can occur at any time; therefore, all FBI personnel should understand and be able to implement basic salvage operations to reduce continued deterioration of FBI records.

Information about protecting and recovering records is available on RMD's Records Protection and Recovery Intranet site.

Damaged FBI records must be reported to RMD through an EC (FD-1057), using case file 319O-HQ-A1487624-XX, Records Management Matters (replace XX with the FO's two-letter designator). The incident that damaged the documents and the remediation provided must be described in the EC.

4.15. RMD Records Disaster Team

The RMD Records Disaster Team is a collaborative effort of trained RMD employees who can deploy to any FBI division for predisaster and postdisaster records assistance. Additional information about the Records Disaster Team can be found on RMD's Records Protection and Recovery Intranet site.

4.16. Vital Records

Vital records are records that are essential to the functions of the FBI's operation during and following an emergency. The loss of these records during a disaster can create gaps in vital information, resulting in the disruption of essential services, exposure to unplanned expenses of financial settlements or loss of revenue, increased vulnerability to litigation, and loss of productivity.

Vital records may be maintained on a variety of media including paper, magnetic tape or disc, photographic film, removable hardware, and microfilm. The Vital Records Program (VRP), as defined in 36 CFR § 1236.14, provides resources to identify, use, and protect the essential operating records needed to meet federal responsibilities under national security or disaster emergencies. The *Vital Records Policy Guide* (0794PG) contains information about the FBI's Vital Records Program.

5. Summary of Legal Authorities

Several agencies, including NARA, OMB, and the General Services Administration (GSA) share oversight of records management in the federal government. Listed below are citations to the codes, regulations, and authorities most relevant to records management:

- Records Management by the Archivist of the United States and by the Administrator of General Services (44 U.S.C. Chapter 29)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)
- Disposal of Records (44 U.S.C. Chapter 33)
- Coordination of Federal Information Policy (44 U.S.C. Chapter 35)
- Public Money, Property, or Records (18 U.S.C. § 641)
- Criminal Penalties for Unauthorized Disposal of Federal Records (18 U.S.C. § 2071)
- The Freedom of Information Act (5 U.S.C. § 552)
- The Privacy Act of 1974 (5 U.S.C. § 552a)
- Federal Records (36 CFR Chapter 12, Subchapter B)
- Personnel Records (5 CFR Part 293)
- OMB Circular A-130: *Management of Federal Information Resources*
- U.S. Office of Personnel Management (OPM) Manual, *The Guide to Personnel Recordkeeping* (November 2006)
- Department of Justice Order No. 0801 (March 12, 2014) (establishes policy governing the DOJ Records and Information Management (RIM) Program for the creation, capture or receipt, maintenance and use, and disposition of all DOJ records"

Appendix A: Final Approvals

POLICY TITLE: *Records Management Policy Guide*	
Primary Strategic Objective	P-1 Streamline administrative and operational processes
Publish Date	2015-06-04
Effective Date	2015-06-04
Review Date	2018-06-04
EXEMPTIONS	
None	
REFERENCES	
See Section 4 and Appendices B and C of this PG.	
APPROVALS	
Sponsoring Executive Approval	**Michelle A. Jupina** Assistant Director Records Management Division
Final Approval	**Kevin L. Perkins** Associate Deputy Director

Appendix B: Sources of Additional Information

- *Declassification of Classified National Security Information Policy Guide* (0623DPG)
- *Domestic Investigations and Operations Guide* (DIOG) (0667DPG)
- *Social Media and Other Electronic Information Sharing Technologies Directive and Policy Guide* (0579DPG)
- *FBI Electronic Recordkeeping Certification Manual*
- *Field Evidence Management Policy Guide* (0780PG)
- *FRAP User Guide for Non-NNCP Users*
- FRAP Intranet site
- PD 0418D, *Freedom of Information Act and Privacy Act Requests*
- PD 0619D, *Legal Hold Policy*
- "Managing Your Federal Records: A Guide for FBI Executives"
- PD 0249, *Metadata Tagging of Electronically Stored Information in FBI Systems*
- Open storage secure area checklist
- *Prepublication Review Policy Guide* (0792PG)
- PD 0423D, *Preservation and Disclosure of Electronic Communications in Federal Criminal Cases*
- Records Management Division Intranet site
- *Records Management User Manual* (RM User Manual)
- RMD Help Desk
- PD 0610D, *Security Incident Program*
- Sentinel Intranet site
- *Indexing User Manual for Sentinel*
- PD 0774D, *Records Management Standards for Scanned Documents*
- PD 0671D, *Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format*
- *Vital Records Policy Guide* (0794PG)
- "Memorandum of Understanding Among the U.S. Office of Personnel Management, the Federal Bureau of Investigation, and the National Archives and Records Administration" and Addendums 1, 2, and 3
- PD 0457D, *RMD Statement of Authorities and Responsibilities*

Appendix C: Acronyms

ACS	Automated Case Support [system]
AD	assistant director
ADIC	assistant director in charge
ARC	Alexandria Records Center
CD	compact disc
CDC	chief division counsel
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services Division
DCPU	Discovery Coordination and Policy Unit
DIOG	*Domestic Investigations and Operations Guide*
DK-RPAS	RMD Records Policy and Administration Section
DocLab	Document Conversion Laboratory
DOJ	Department of Justice
DVD	digital video discs
EC	electronic communication
EIST	electronic information sharing technologies
ELSUR	electronic surveillance
e-mail	electronic mail
EO	executive order
eOPF	electronic official personnel file
ERK	electronic recordkeeping
ERKC	electronic recordkeeping certification

Exec Sec	Executive Secretariat
FACS	file automated control system
fax	facsimile
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FBINet	Federal Bureau of Investigation Network
FO	field office
FOIA	Freedom of Information Act
FOIPA	Freedom of Information and Privacy Acts
FRAP	file request automation report
FTI	federal tax information
GRS	General Records Schedule
GSA	General Services Administration
INSD	Inspection Division
IP	Internet Protocol
IT	information technology
ITB	Information and Technology Branch
ITID	Information Technology Infrastructure Division
JEH	J. Edgar Hoover [Building]
KM	knowledge management
Legat	legal attaché
LEO	Law Enforcement Online

MAOP	*Manual of Administrative Operations and Procedures*
NARA	National Archives and Records Administration
NNCP	National Name Check Program
OGA	other government agency
OGC	Office of the General Counsel
OGS	other government service
OMB	Office of Management and Budget
OO	office of origin
OPF	official personnel files
OPM	Office of Personnel Management
OPR	Office of Professional Responsibility
PACU	Policy, Analysis, and Compliance Unit
PAR	performance appraisal reports
PCO	permanent charge–out
PD	policy directive
PG	policy guide
RA	resident agency
RAS	Records Automation Section
RDU	Records Disposition Unit
RIDS	Record/Information Dissemination Section
RM	Records Manual
RMA	records management application

RMAU	Records Management Application Unit
RMD	Records Management Division
RMT	Record Marking Tool
RPAS	Records Policy and Administration Section
RSMU	Records Storage and Maintenance Unit
SA	special agent
SAC	special agent in charge
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SecD	Security Division
SF	Standard Form
SIRS	Security Incident Reporting System
TS	TOP SECRET
TSU	Training Services Unit
U.S.C.	United States Code
UNet	unclassified network
USG	United States government
VRP	Vital Records Program

Appendix D: Contact Information

Records Management Division	
RMD Help Desk phone	[redacted]
RMD Help Desk e-mail	[redacted]

b7

Appendix E: Supersessions

This PG supersedes:

- *Records Management Manual* (POL05-0001-RMD)
- PD 0106D, *Reporting Missing Files and Serials*
- PD 0108D, *Disposition Authority for FBI Records*
- PD 0291D, *Supervisory Approval of Administrative Records*
- PD 0332D, *Use of Special Characters and Symbols as Subfile Designators*
- PD 0372D, *Non-record E-mail Retention*
- PD 0131D, *Modification and Destruction of Records*
- 66F-HQ-A1358157-POLI serial 2
- 319W-HQ-A1487698 serial 12
- 319W-HQ-A1487698 serial 325
- 319O-HQ-1487624 serial 545
- *Manual of Administrative Operations and Procedures* (MAOP) Part 1 Section 20-4.1. through 20-4.2.
- MAOP Part 2 Section 2-3.5.
- MAOP Part 2 Section 2-3.11.
- MAOP Part 2 Section 2-4.1. through 2-4.3.8.
- MAOP Part 2 Section 2-4.5. through 2-4.5.29.
- MAOP Part 2 Section 2-5.1. through 2-5.3.1.
- MAOP Part 2 Section 11-5.1.
- MAOP Part 2 Section 11-7.3.